VERIFICATION OF TRANSLATION

I, Tomoko Hara, translator of 6F, Yodogawa 5-Bankan, 3-2-1, Toyosaki, Kita-ku, Osaka, Japan, hereby declare that I am conversant with the English and Japanese languages and am a competent translator thereof. I further declare that to the best of my knowledge and belief the following is a true and correct translation made by me of the English translation of claims of Japanese Patent Application No. 2006-519466 filed to the Japanese Patent Office on December 20, 2007.

Date: February 20, 2008

原 朋子

TOMOKO HARA

CLAIMS

1. A data processing device for playing back a digital work recorded on a recording medium having also recorded (i) a plurality of record digest values generated from a plurality of data blocks constituting the digital work and (ii) record signature data generated by applying, with use of a signature key, a signature generating algorithm to a first combination made of some or all of the plurality of record digest values, comprising:

a verification key storing unit storing a verification key corresponding to the signature key;

a using unit operable to play back the digital work;

a selecting unit operable to randomly select a predetermined number of data blocks from the plurality of data blocks;

a calculating unit operable to calculate a plurality of calculation digest values from the selected data blocks;

a reading unit operable to read remaining record digest values corresponding to unselected data blocks from among the plurality of record digest values;

a generating unit operable to generate a second combination based on calculation digest values and the remaining record digest values, the second combination being same as data which is generated from the first combination by replacing record digest values corresponding to the selected data blocks with corresponding calculation digest values;

a signature verifying unit operable to perform a signature verification by applying, with use of the verification key, a signature verification algorithm to the second combination and the record signature data; and

a use controlling unit operable to stop the using unit from playing back the digital work when the signature verification is unsuccessful.

2. The data processing device of Claim 1, wherein

the plurality of record digest values include a plurality of primary record digest values, each of which is generated for one of the plurality of data blocks, and a plurality of secondary record digest values generated from two or more of the plurality of primary record digest values, and the record signature data is generated by applying, with use of the signature key, the signature generating algorithm to the first combination made of some or all of the plurality of secondary record digest values,

the reading unit reads, from the recording medium, the plurality of secondary record digest values and the remaining record digest values from among the plurality of primary record digest values, and

the generating unit includes:

a calculating subunit operable to calculate one or more secondary calculation digest values based on the calculation digest values and the remaining record digest values; and

a combining subunit operable to generate the second combination based on the plurality of secondary record digest values and the one or more secondary calculation digest values, the second combination being same as data which is generated from the first combination by replacing record digest values corresponding to the selected data blocks with corresponding calculation digest values.

3. The data processing device of Claim 2, wherein

the digital work includes a plurality of files, each of which corresponds to one of the plurality of secondary record digest values and is constituted by two or more of the plurality of data blocks,

each of the plurality of secondary record digest values is generated by using primary record digest values corresponding one-to-one with the two or more of the plurality of data blocks constituting a file corresponding to the secondary record digest value,

the calculating subunit calculates a secondary calculation digest value, with respect to each file including at least one of the selected data blocks, by using primary record digest values corresponding to the unselected data blocks included in the file and the calculation digest value corresponding to the at least one of the selected data blocks,

the reading unit reads, with respect to each file including none of the selected data blocks, a secondary record digest value corresponding to the file, and

the combining subunit generates the second combination by combining the calculated secondary calculation digest values and the read secondary record digest values.

4. The data processing device of Claim 3, wherein

the plurality of record digest values are hash values each generated by a hash function,

the calculating unit applies the hash function to each of the selected data blocks in order to calculate hash values which are the calculation digest values, and

the calculating subunit applies the hash function to the primary

record digest values corresponding to the unselected data blocks and the calculation digest values in order to calculate hash values which are the secondary calculation digest values.

5. The data processing device of Claim 3, comprising, instead of the use controlling unit:

a warning display unit operable to display, when the digital work is judged as not being valid, a notice of invalidity of the digital work.

6. The data processing device of Claim 1 wherein the recording medium has additionally recorded (i) area information indicating an access permitted area, on the recording medium, that an external device is permitted to access and (ii) signature data generated by applying, with use of a signature key, the signature generating algorithm to part or all of the digital work and the area information, the data processing device further comprising:

an access prohibiting unit operable to prohibit access to areas other than the access permitted area based on the area information;

a second verifying unit operable to perform a signature verification by applying, with use of a verification key, a signature verification algorithm to the digital work, the area information, and the signature data; and

a second use controlling unit operable to stop the using unit from playing back the digital work when the signature verification is unsuccessful.

7. The data processing device of Claim 1, wherein

the selecting unit, the calculating unit, the reading unit, and the signature verifying unit are assembled together in a single large scale integration.

8. The data processing device of Claim 1, wherein

the reading unit reads record digest values corresponding to the selected data blocks from the recording medium, and

the data processing device further comprising:

a digest value verifying unit operable to make a judgment whether the plurality of record digest values recorded on the recording medium match calculation digest values; and

a third use controlling unit operable to stop the using unit from playing back the digital work when the judgment is affirmative.

9. A recording medium used with the data processing device of Claim 1,

(i) having recorded thereon:

a digital work;

a plurality of record digest values generated from a plurality of data blocks constituting the digital work; and

record signature data generated based on the plurality of record digest values, and

(ii) supplying to the data processing device the digital work, the plurality of record digest values, and the record signature data.

10. A data processing method (i) applied to a data processing device including: a verification key storage unit storing a verification key corresponding to a signature key; a using unit; a selecting unit; a

calculating unit; a reading unit; a generating unit; a signature verifying unit; and a user control unit, and reading a digital work from a recording medium having recorded thereon: the digital work; a plurality of record digest values generated from a plurality of data blocks constituting the digital work; record signature data generated by applying, with use of a signature key, a signature generating algorithm to a first combination made of some or all of the plurality of record digest values, the data processing method comprising:

a using step of causing the using unit to play back the digital work;

a selecting step of causing the selecting unit to randomly select a predetermined number of data blocks from the plurality of data blocks;

a calculating step of causing the calculating unit to calculate a plurality of calculation digest values from the selected data blocks;

a reading step of causing the reading unit to read remaining record digest values corresponding to unselected data blocks from among the plurality of record digest values;

a generating step of causing the generating unit to generate a second combination based on calculation digest values and the remaining record digest values, the second combination being same as data which is generated from the first combination by replacing record digest values corresponding to the selected data blocks with corresponding calculation digest values;

a signature verifying step of causing the signature verifying unit to perform a signature verification by applying, with use of the verification key, a signature verification algorithm to the second combination and the record signature data; and

a use controlling step of causing the use controlling unit to stop the using unit from playing back the digital work when the signature verification is unsuccessful.

11. A data processing program (i) applied to a data processing device including: a verification key storage unit storing a verification key corresponding to a signature key; a using unit; a selecting unit; a calculating unit; a reading unit; a generating unit; a signature verifying unit; and a user control unit, and reading a digital work from a recording medium having recorded thereon: the digital work; a plurality of record digest values generated from a plurality of data blocks constituting the digital work; record signature data generated by applying, with use of a signature key, a signature generating algorithm to a first combination made of some or all of the plurality of record digest values, the data processing program causing the data processing device to execute:

a using step of causing the using unit to play back the digital work;

a selecting step of causing the selecting unit to randomly select a predetermined number of data blocks from the plurality of data blocks;

a calculating step of causing the calculating unit to calculate a plurality of calculation digest values from the selected data blocks;

a reading step of causing the reading unit to read remaining record digest values corresponding to unselected data blocks from among the plurality of record digest values;

a generating step of causing the generating unit to generate a second combination based on calculation digest values and the remaining

record digest values, the second combination being same as data which is generated from the first combination by replacing record digest values corresponding to the selected data blocks with corresponding calculation digest values;

a signature verifying step of causing the signature verifying unit to perform a signature verification by applying, with use of the verification key, a signature verification algorithm to the second combination and the record signature data; and

a use controlling step of causing the use controlling unit to stop the using unit from playing back the digital work when the signature verification is unsuccessful.

12. The data processing program of Claim 11 recorded on a computer-readable recording medium.

【書類名】 手続補正書
【整理番号】 2048165160
【提出日】 平成19年12月20日
【あて先】 特許庁長官 殿
【事件の表示】
【出願番号】 特願2006-519466
【補正をする者】
【識別番号】 000005821
【氏名又は名称】 松下電器産業株式会社
【代理人】
【識別番号】 100090446
【弁理士】
【氏名又は名称】 中島 司朗
【発送番号】 535882
【手続補正1】
【補正対象書類名】 特許請求の範囲
【補正対象項目名】 全文
【補正方法】 変更
【補正の内容】
【書類名】特許請求の範囲
【請求項１】
デジタル著作物と、前記デジタル著作物を構成する複数のデータブロックから生成された複数の記録要約値と、複数の記録要約値からなる第１結合物に対して署名鍵を用いた署名生成アルゴリズムを施すことで生成された記録署名データとを記録している記録媒体から、前記デジタル著作物を読み出して再生するデータ処理装置であって、
前記署名鍵に対応する検証鍵を保持する検証鍵保持手段と、
前記記録媒体に記録されている前記デジタル著作物を再生する利用手段と、
前記データブロックからランダムに所定数個の選択データブロックを選択する選択手段と、
各選択データブロックから、演算要約値を算出する演算手段と、
前記記録媒体に記録されている記録要約値群から、少なくとも、前記選択データブロックを除く他のデータブロックに対応する残存要約値を読み出す読出手段と、
前記演算要約値及び前記残存要約値から、前記第１結合物のうち、前記選択データブロックに対応する記録要約値を前記演算要約値に置き換えたデータである第２結合物を生成する生成手段と、
生成された前記第２結合物と前記記録署名データとに、前記検証鍵を用いた署名検証アルゴリズムを施すことによって署名検証を行う署名検証手段と、
前記署名検証手段による署名検証が失敗した場合に、前記デジタル著作物の再生を停止する利用制御手段と
を含むことを特徴とするデータ処理装置。
【請求項２】
前記記録媒体に記録されている記録要約値群は、各データブロックに対して生成された一次記録要約値と、複数の一次記録要約値から生成された複数の二次記録要約値とからなり、前記記録署名データは、前記複数の二次記録要約値からなる前記第１結合物に対して前記署名鍵を用いた前記署名生成アルゴリズムを施すことで生成されたものであり、
前記読出手段は、前記記録媒体から、前記一次記録要約値群のうち前記選択データブロックを除く他のデータブロックに対応する前記残存要約値と、前記二次記録要約値とを読み出し、
前記生成手段は、
前記演算要約値及び前記残存要約値に基づいて、１個以上の二次演算要約値を算出する

算出部と、
前記二次記録要約値と前記二次演算要約値とから、前記第１結合物のうち、前記選択データブロックに対応する一次記録要約値から生成された二次記録要約値を、前記二次演算要約値に置き換えたデータである前記第２結合物を生成する結合部とを備える
ことを特徴とする請求項１に記載のデータ処理装置。
【請求項３】
前記記録媒体に記録されている前記デジタル著作物は、複数個のファイルから構成され、各ファイルは、二次記録要約値に対応し、複数のデータブロックから構成され、
各二次記録要約値は、対応するファイルを構成する複数のデータブロックのそれぞれに対する一次記録要約値を用いて生成され、
前記生成手段の算出部は、
選択された選択データブロックを含む各ファイルについて、当該ファイルに含まれるデータブロックのうち当該選択データブロックを除く残存データブロックに対応する一次記録要約値と、当該選択データブロックに対応する演算要約値とを用いて、前記二次演算要約値を算出し、
前記読出手段は、選択された選択データブロックを含まない各ファイルについて、当該ファイルに対応する二次記録要約値を読み出し、
前記結合部は、算出された二次演算要約値と読み出した二次記録要約値を結合した前記第２結合物を生成する、
ことを特徴とする請求項２のデータ処理装置。
【請求項４】
各要約値は、ハッシュ関数により生成されたハッシュ値であり、
前記演算手段は、各選択データブロックにハッシュ関数を施して、ハッシュ値を算出し、算出したハッシュ値を前記演算要約値とし、
前記算出部は、一次記録要約値と演算要約値とに、ハッシュ関数を施して、ハッシュ値を算出し、算出したハッシュ値を前記二次演算要約値とする
ことを特徴とする請求項３のデータ処理装置。
【請求項５】
前記利用制御手段に代えて、前記デジタル著作物が不正であると判断される場合に、その旨を表示する警告表示手段を備える
ことを特徴とする請求項３に記載のデータ処理装置。
【請求項６】
デジタル著作物と、外部機器によるアクセスが許可される当該記録媒体上の許可領域を示す領域情報と、前記デジタル著作物及び前記領域情報とに対して署名鍵を用いた署名生成アルゴリズムを施すことで生成された署名データとを記録している記録媒体から前記デジタル著作物を読み出して利用するデータ処理装置であって、
前記領域情報に基づいて、前記許可領域外へのアクセスを禁止するアクセス禁止手段と、
前記デジタル著作物と前記領域情報と前記署名データとに、前記署名鍵に対応する前記検証鍵を用いた署名検証アルゴリズムを施すことによって署名検証を行う第２検証手段と、
前記署名検証に失敗すると、前記デジタル著作物の再生を停止する第２利用制御手段
とを備えることを特徴とする請求項１に記載のデータ処理装置。
【請求項７】
前記選択手段、前記演算手段、前記読出手段及び前記署名検証手段は、１個の大規模集積回路から構成されている
ことを特徴とする請求項１のデータ処理装置。
【請求項８】
請求項１のデータ処理装置であって、
前記読出手段は、さらに、前記記録媒体から前記選択データブロックに対応する前記記

録要約値を読み出し、
前記データ処理装置は、さらに、
前記記録媒体に記録されている前記記録要約値と前記演算要約値とが一致するかどうかを検証する要約値検証手段と、
前記要約値検証手段による検証の結果、一致しないと判断される場合に、前記デジタル著作物の再生を停止する第３利用制御手段とを
備えることを特徴とする請求項１のデータ処理装置。
【請求項９】
記録媒体であって、請求項１に記載のデータ処理装置と共に用いられ、
デジタル著作物と、前記デジタル著作物を構成する複数のデータブロックから生成された複数の記録要約値と、前記記録要約値群に基づいて生成された記録署名データとを記憶し、
前記データ処理装置に対して、前記著作物データと前記記録要約値と前記記録署名データとを供給する
ことを特徴とする記録媒体。
【請求項１０】
署名鍵に対応する検証鍵を保持する検証鍵保持手段と、利用手段と、選択手段と、演算手段と、読出手段と、生成手段と、署名検証手段と、利用制御手段とを備えるデータ処理装置に適用され、デジタル著作物と、デジタル著作物を構成する複数のデータブロックから生成された複数の記録要約値と、複数の記録要約値からなる第１結合物に対して署名鍵を用いた署名生成アルゴリズムを施すことで生成された記録署名データとを記録している記録媒体から、前記デジタル著作物を読み出して利用するデータ処理方法であって、
前記利用手段により、前記記録媒体に記録されている前記デジタル著作物を再生する利用ステップと、
前記選択手段により、前記データブロックからランダムに所定数個の選択データブロックを選択する選択ステップと、
前記演算手段により、各選択データブロックから、演算要約値を算出する演算ステップと、
前記読出手段により、前記記録媒体に記録されている記録要約値群から、前記選択データブロックを除く他のデータブロックに対応する残存要約値を読み出す読出ステップと、
前記生成手段により、前記演算要約値及び前記残存要約値から、前記第１結合物のうち、前記選択データブロックに対応する記録要約値を前記演算要約値に置き換えたデータである第２結合物を生成する生成ステップと、
前記署名検証手段により、生成された前記第２結合物と前記記録署名データとに、前記検証鍵を用いた署名検証アルゴリズムを施すことによって署名検証を行う署名検証ステップと、
前記利用制御手段により、前記署名検証手段による署名検証が失敗した場合に、前記デジタル著作物の再生を停止する利用制御ステップと
を含むことを特徴とするデータ処理方法。
【請求項１１】
署名鍵に対応する検証鍵を保持する検証鍵保持手段と、利用手段と、選択手段と、演算手段と、読出手段と、生成手段と、署名検証手段と、利用制御手段とを備えるデータ処理装置に適用され、デジタル著作物と、デジタル著作物を構成する複数のデータブロックから生成された複数の記録要約値と、複数の記録要約値からなる第１結合物に対して署名鍵を用いた署名生成アルゴリズムを施すことで生成された記録署名データとを記録している記録媒体から、前記デジタル著作物を読み出して利用するデータ処理プログラムであって、
前記利用手段により、前記記録媒体に記録されている前記デジタル著作物を再生する利用ステップと、
前記選択手段により、前記データブロックからランダムに所定数個の選択データブロッ

クを選択する選択ステップと、
前記演算手段により、各選択データブロックから、演算要約値を算出する演算ステップと、
前記読出手段により、前記記録媒体に記録されている記録要約値群から、前記選択データブロックを除く他のデータブロックに対応する残存要約値を読み出す読出ステップと、
前記生成手段により、前記演算要約値及び前記残存要約値から、前記第１結合物のうち、前記選択データブロックに対応する記録要約値を前記演算要約値に置き換えたデータである第２結合物を生成する生成ステップと、
前記署名検証手段により、生成された前記第２結合物と前記記録署名データとに、前記検証鍵を用いた署名検証アルゴリズムを施すことによって署名検証を行う署名検証ステップと、
前記利用制御手段により、前記署名検証手段による署名検証が失敗した場合に、前記デジタル著作物の再生を停止する利用制御ステップと
を含むことを特徴とするデータ処理プログラム。
【請求項１２】
前記データ処理プログラムは、コンピュータ読み取り可能な記録媒体に記録されていることを特徴とする請求項１１に記載のデータ処理プログラム。

【手続補正2】
【補正対象書類名】 明細書
【補正対象項目名】 ０００６
【補正方法】 変更
【補正の内容】
【０００６】
上記の目的を達成するために、本発明は、デジタル著作物と、前記デジタル著作物を構成する複数のデータブロックから生成された複数の記録要約値と、複数の記録要約値からなる第１結合物に対して署名鍵を用いた署名生成アルゴリズムを施すことで生成された記録署名データとを記録している記録媒体から、前記デジタル著作物を読み出して再生するデータ処理装置であって、前記署名鍵に対応する検証鍵を保持する検証鍵保持手段と、前記記録媒体に記録されている前記デジタル著作物を再生する利用手段と、前記データブロックからランダムに所定数個の選択データブロックを選択する選択手段と、各選択データブロックから、演算要約値を算出する演算手段と、前記記録媒体に記録されている記録要約値群から、少なくとも、前記選択データブロックを除く他のデータブロックに対応する残存要約値を読み出す読出手段と、前記演算要約値及び前記残存要約値から、前記第１結合物のうち、前記選択データブロックに対応する記録要約値を前記演算要約値に置き換えたデータである第２結合物を生成する生成手段と、生成された前記第２結合物と前記記録署名データとに、前記検証鍵を用いた署名検証アルゴリズムを施すことによって署名検証を行う署名検証手段と、前記署名検証手段による署名検証が失敗した場合に、前記デジタル著作物の再生を停止する利用制御手段とを含むことを特徴とする。